Association for Information Systems
AIS Electronic Library (AISeL)

PACIS 2016 Proceedings

Pacific Asia Conference on Information Systems (PACIS)

Summer 6-27-2016

ADOPTION INTENTION ON CLOUD STORAGE SERVICES: THE ROLE OF TECHNOLOGY TRUST, PRIVACY AND SECURITY CONCERNS

Kuo-Chung Chang
Yuan Ze University, changkc@saturn.yzu.edu.tw

Yoke May Seow
Yuan Ze University, s999203@mail.yzu.edu.tw

ADOPTION INTENTION ON CLOUD STORAGE SERVICES: THE ROLE OF TECHNOLOGY TRUST, PRIVACY AND SECURITY CONCERNS

Kuo-Chung Chang, Department of Information Management, Yuan Ze University, Taiwan R.O.C., changkc@saturn.yzu.edu.tw

Yoke May Seow, Department of Information Management, Yuan Ze University, Taiwan R.O.C., s999203@mail.yzu.edu.tw

Abstract

Cloud storage is getting increasing attention in the last few years. By moving data to location-transparent centralized facilities or providers, cloud storage services offer significant economic advantages to consumers and enterprises. However, concerns have been raised regarding the duplication, dissemination, and deletion of data stored on the cloud. In addition, data leakage would be another major concern whether accidental or due to a malicious hacker attack. Thus, the formation of trust in technology is particularly essential for users to cope with the uncertainty of information privacy because users relinquish their ultimate control over the fate of their data. Trust in technology involves two major trusting mechanisms, namely cognitive trust and emotional trust. Cognitive trust, which is also known as trusting belief, refers to the users' rational expectations that the technology under scrutiny will have the necessary attributes to rely on. Three features of cognitive trust have been considered as essential elements for cloud storage applications namely, openness, consent, and access. Meanwhile, emotional trust refers to users' feeling of security and comfort to rely on the technology in use. It contains three different components, namely competence, relatedness, and autonomy. A model is proposed to depict the relationship between technology trust, perceived information privacy and security concerns. This research extends trust research on information privacy and information security concerns and enrich existing literature on the formation of trust. The results of this research could provide specific technology traits that vendors can adopt in to build up users' trust in the technology.

Keywords: cloud storage services, technology trust, cognitive trust, emotional trust, information privacy concerns, information security concerns

1 INTRODUCTION

Cloud storage is getting increasing attention in the last few years. By moving data to location-transparent centralized facilities or providers, cloud storage services offer significant economic advantages to consumers and enterprises. This change toward cloud storage brings appealing benefits, such as on-demand self-service, ubiquitous network access, location-independent resource pooling, rapid resource elasticity, and usage-based pricing (Mell & Grance, 2011). Despite the significant benefits offered, cloud storage raises serious challenges to users' outsourced information. Concerns have been raised regarding the duplication, dissemination, and deletion of data stored on cloud storage services (Caldwell, 2012). In addition, data leakage would be another major concern whether accidental or due to a malicious hacker attack. Consequently, users may refrain completely from using cloud storage resulting from security and privacy concerns. Thus, mitigating perceived risks due to information privacy and security concerns becomes an essential task for the perpetual growth of cloud storage services.

One way to mitigate perceived risks is by increasing users' trust in technology that makes cloud storage possible. Trust has been studied in various scientific disciplines and accepted as fundamental component of human social relations. This present study focuses particularly on trust in cloud storage services which is defined as the willingness of users to depend on cloud storage technology under uncertain conditions (McKnight et al., 2011). The formation of trust in technology is essential for users to cope with the uncertainty about information privacy because users relinquish their ultimate control over the fate of their data. Therefore, this study argues that for users to adopt cloud storage services, it is noteworthy to determine what makes the technology itself trustworthy.

The main goal of this proposal is to derive understanding on how trust in technology is built and how to overcome adoption barriers due to privacy concerns. This study aims to address the following questions: 1) what antecedents influence users' trust in a cloud storage context? and 2) what impact does trust have in cloud storage applications with regards to users' privacy concerns and their adoption of applications? To address these questions, a research model is developed to examine how users could be motivated to trust technology and how it influences the adoption of cloud storage services. Trust in technology is not a unidimensional but a multi-dimensional concept (Komiak and Benbasat, 2006). Drawing on past trust research from the information systems (IS) domain (Bui et al., 2013; Komiak and Benbasat, 2006; McKnight et al., 2011), this current research contends that to build up users' trust in cloud storage technologies, it requires a combination of cognitive trust and emotional trust. This is based on the assumption that trust decisions usually involve both reasoning and feeling (Gefen, 2003; Komiak and Benbasat, 2006; McKnight et al. 2002).

2 LITERATURE REVIEW AND THEORETICAL FOUNDATIONS

2.1 Cognitive trust (trusting belief) in technology

Cognitive trust, also known as trusting belief, reflects beliefs that the technology has the necessary attributes to perform as expected in a situation (McKnight et al., 2011). It involves users' rational expectation that the technology is reliable to complete specific tasks. In the current context, trust represents the beliefs that the cloud storage technology possesses the traits that can protect users' information privacy. Prior studies posited that IT users have an overall technology trusting expectation

that is composed of separate, yet related expectations. Three system-like technology trusting attributes with regards to users' preference to trust technology are proposed, namely openness, consent, and access (Hong and Landay, 2004; Jiang et al. 2002; Langheirnrich, 2001, 2002).

Openness refers to technological features that make the information about collection, use, and disclosure of personal information available to the users. For example, when privacy policy is made known to the users, it provides announcement mechanisms. Consent refers to the individual's free and specific permission for the collection, use or disclosure of personal information. For instance, opt in/out mechanisms are provided that involve the subject of personal information in deciding the authorization of the collection, transmission, and disclosure of personal information. Access entails mechanisms that provide users to access to their personal information and informed of its uses and disclosure. For example, systems could provide feedback on what personal information is being stored. These mechanisms can empower users to challenge the accuracy and completeness of the information and have it amended.

2.2 Emotional trust in technology

Emotional trust is defined as the extent that the users feel secure and comfortable to rely on the technology studied (Komiak and Benbasat, 2006). Though emotional trust has been proposed as an important element in trust formation process, its structure has not been revealed because emotion is difficult to be analyzed or assessed. Drawing from self-determination theory (SDT), this study postulates that emotional trust has three components, namely autonomy, competence, and relatedness. SDT proposes that individuals strive to satisfy their basic psychological needs. According to SDT, autonomy, competence, and relatedness are three basic psychological needs that are the essential basis for predicting the quality of behavior and experience within a specific situation (Ryan and Deci, 2002). Satisfaction of these three basic needs underlie natural inclinations towards engaging in discretionary behaviors such as adopting a particular cloud storage service.

In SDT, perceived autonomy is conceptualized as the experienced sense of choice, volition and freedom from excessive external pressure toward behaving or thinking a certain way (Ryan and Deci, 2000). Put it differently, autonomous individuals experience psychological freedom and ownership of their actions. Perceived autonomy refers not to being independent, detached, or selfish but rather to the feeling of volition that can accompany any act. For example, individuals may experience autonomy satisfaction when they depend on others or when they follow others' requests, as long as a there is meaningful rationale for doing so (Soenens et al., 2007). An individual who feels autonomous perceives that the behavior is self-chosen and endorsed. Thus, when less autonomous, the person feels that his/her behavior is compelled or controlled. Perceived competence refers to feeling effective in one's ongoing interaction with the environment and experiencing opportunities to exercise and express one's capacities (Ryan and Deci, 2002). It is analogous to self-efficacy, i.e., beliefs in one's ability to perform activities. When individuals feel competent, they feel confident that they are capable of accomplishing the behavioral outcome. Though perceived competence refers to an affective experience of effectiveness which results from mastering a task, perceived competence is not regarded as attained skills or capabilities, but rather as a subjective perception of confidence and efficacy to interact effectively with the environment that may or may not correspond to his or her actual competence (Ryan and Deci, 2002). Perceived relatedness refers to feeling respected and cared for by others (Sheldon et al., 2003). It reflects the innate desires to be supported by others when engaging in behaviors. Here, perceived relatedness involves social support that provides a milieu in which an individual feels fairly treated and experiences respect and value when connecting to the environment where individuals interact with other social entities (Baumeister and Leary, 1995; Ryan and Deci,

2002). This sense of relatedness affords a person's "secure base" to engage in a particular environment.

2.3 Information privacy and security concerns

Information privacy and security concerns are primary barriers to the adoption of cloud storage services and must be mitigated. Privacy concerns refer to the worries about the loss of their personal information (Malhotra et al., 2004). Specifically, people are concerned about unauthorized or improper collection, access and secondary use of personal information, and errors in information (Malhotra et al., 2004). This control perspective of information privacy is by far the most dominant view in privacy research (Smith et al., 2011) and is adopted in the current study. Information security concerns, on the other hand, deals with users' beliefs that the service provider is unable or unwilling to safeguard their personal information from security breaches during transmission and storage (Pavlou et al., 2007). Security concerns increase perceived uncertainties in online services, leading to users' unwillingness to adopt those services. Although information privacy and security are very closely related, their concepts are different which have been distinguished in several empirical studies (e.g., Pavlou et al., 2007; Shin, 2010).

3 RESEARCH MODEL AND HYPOTHESES

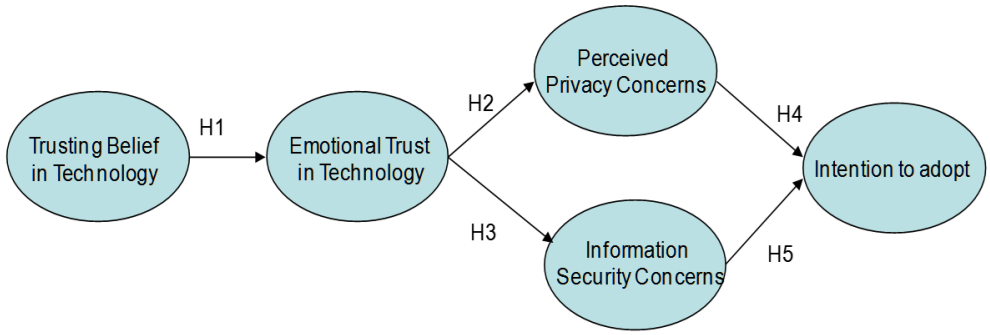

Figure 1. Research model

3.1 Trusting belief and emotional trust

This study posits that trusting belief is positively associated with emotional trust. Technology enabling cloud storage systems characterizing openness, consent, and access control enhances a user's perceived competence, autonomy, and relatedness in manipulating personal information. According to the SDT (Ryan and Deci, 2000), technology providing features attributing to openness, consent, and feedback that safeguard personal information will lead to feelings of increased competence (Hein and Koka, 2007). Such features enable the users to clearly see the links between their actions and valence of outcomes, and evaluate the likelihood of certain actions leading to expected outcomes. Consent features (e.g., opt-in or opt-out options) provide meaningful information in a non-manipulative manner and offering opportunities for choice (Deci et al. 1994). Finally, trustworthy technology allows users to develop secure attachment (or dependence) relationship with those technologies that will increase users' confidence and decrease their anxiety when performing tasks. Hence, we postulate:

H1: Technology trust belief is positively associated with emotional trust.

3.2 Emotional trust and perceived privacy concerns

This study posits that emotional trust is negatively associated with perceived privacy concerns. When users feel competent, they experience self-efficacy and confidence in themselves. In the context of technology usage, users with high perceived competent in technologies feel less helpless and instill their confidence in manipulating the intelligent environment and restrict the extent of privacy intrusion. Individuals with high relatedness satisfaction experience a sense of security during the exchange of personal information. Prior studies discovered that the sense of security can be achieved through various assurance mechanisms (e.g., institutional or technological) offered by service providers to assure users that efforts have been devoted to protect personal information (Culnan and Bies, 2003). With these assurance mechanisms, a sense of security and safety is likely to be developed because users feel that the technology will not exploit their personal information; thus reducing the risk of personal information disclosure (Pavlou et al., 2007). Individuals with high perceived autonomy experience less perceived privacy concerns. This is because autonomous individuals experience the feeling of being in control of one's actions. When users feel psychologically less compelled to disclose their personal information and experience a sense of meaning in what they do, concerns on privacy infringement will decrease. Accordingly, we propose:

H2: Emotional trust in cloud storage services is negatively associated with perceived privacy concerns.

3.3 Emotional trust and information security concerns

Information security concerns is defined as the subjective probability in which users believe that their personal information will not be viewed, stored or manipulated by the cloud storage technology in a manner consistent with their confident expectation. This definition captures a personal anticipation rather than an objective measurement and denotes an intuitive perception for assessing risk. Cloud storage users who provide personal information while using the cloud storage technology assume the risk of having this information endangered. Trust is therefore proposed to reduce information security concerns (Kim et al., 2008; Pavlou et al., 2007). When users feel that they are competent in controlling the technology, they are less concerned about personal information being inappropriately manipulated. Likewise, when users' experience that they have the volition to choose how their personal information is managed and feel that their personal information is being cared for from improper access by the technology engaged, they are less concerned about the security of their personal information. We thus hypothesize:

H3: Emotional trust in cloud storage technology is negatively associated with information security concerns.

3.4 Perceived privacy concerns and adoption intention

Perceived privacy concerns gives rise to the lack of control over how personal information will be managed. The higher the privacy concerns that users' experiences, the users will perceive higher uncertainty. As a result, users are less certain about how the technology can safeguard their personal information from improper collection and use. As such, the use of technology can be potentially harmful to users. If users are worried about how the personal information will be handled by the technology, they are unlikely to adopt the cloud storage services. Thus, we posit:

H4: Perceived privacy concerns is negatively associated with the intention to adopt cloud storage services.

3.5 Information security concerns and adoption intention

Information security concerns relate to both hidden information and hidden action. Cloud storage technology is exposed to many security vulnerabilities due to its inherent ubiquity and unobtrusive nature. To adopt cloud storage services, users must be confident in the ability of the technology that cloud storage service providers employ to safeguard their personal information. Information security concerns lead to uncertainty on technology quality, which stems from the users' difficulties in assessing the technology's ability to safeguard information. Hence, users cannot accurately appraise if their personal information will be appropriately safeguarded from security breaches. Thus, we hypothesize:

H5: Information security concerns is negatively associated with the intention to adopt cloud storage services.

4 RESEARCH METHOD

A survey design will be selected to collect data and test the proposed model. The unit of analysis in this study is at the individual level. The key respondents will be users of cloud storage services who are employed in various organizations in Taiwan. The literature reviewed and related constructs are derived from the same level of analysis. This study will systematically follow the steps to first develop the construct validity and reliability of the key concepts included in the research model, and then test the nomological relationships. In terms of construct development and refinement, this study will adopt Moore and Benbasat's (1991) scale development framework as illustrated in Figure 2.

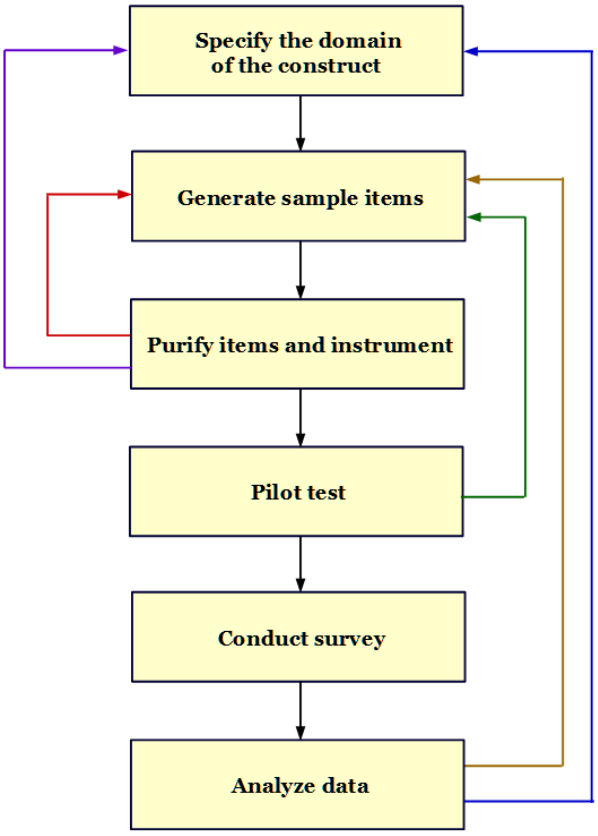

Figure 2. Scale development and research procedures

5 POTENTIAL CONTRIBUTIONS

5.1 Research implications

- Extend trust research on information privacy and information security concerns, particularly focusing on trust in technology due to the unique characteristics of the technology that make the cloud storage services possible.
- Enrich existing literature on the formation of trust: A process model is developed in which trust formation involves in two major mechanisms - cognitive trust and emotional trust.
- By applying the SDT, a new measurement instrument for emotional trust will be developed.

5.2 Practical implications

- Provide specific technology traits that vendors can adopt in order to build up users' trust in the technology.
- Provide a theoretical basis on how cloud storage vendors can build up technology trust to enhance cloud services' adoption by mitigating users' information privacy and security concerns.

References

Baumeister, R.F., and Leary, M. R. 1995. "The need to belong: Desire for interpersonal attachments as a fundamental human motivation," Psychological Bulletin, 117:3, 497-529.

Bui, S., Kettinger, W., and Park, I. 2013. "Personalization to new website users: The role of trust and culture," Proceedings of the 19th American Conference on Information Systems, Chicago, Illinois, August 15-17.

Caldwell, T. 2012. "Locking down the e-wallet," Computer Fraud and Security, 2012:4, 5-8.

Deci, E.L., Eghrari, H., Patrick, B.C., and Leone, D. R. (1994). "Facilitating internalization: The self-determination theory perspective," Journal of Personality, 62:1, 119-142.

Gefen, D., Karahanna, E., and Straub, D.W. 2003. "Trust and TAM in online shopping: An integrated model," MIS Quarterly, 27:1, 51-90.

Hein, V., and Koka, A. 2007. "Perceived Feedback and Motivation in Physical Education and Physical activity," In *Intrinsic Motivation and Self-Determination in Exercise and Sport*, Hagger M. S. and Chatzisarantis, N. L.D. (ed.). Champaign, IL: Human Kinetics.

Hong, J.I. and Landay J.A. 2004. "An architecture of privacy-sensitive ubiquitous computing," Proceedings of the 2nd International Conference on Mobile systems, applications, and services, Boston, Massachusetts, USA. 177-189.

Jiang, X., Hong, J. I., and Landay, J. A. 2002. "Approximate information flows: Socially-based modeling privacy in ubiquitous computing," Lecture Notes in Computer Science, 2498, 176-193.

Komiak, S.Y.X., and Benbasat, I. 2006. "The effects of personalization and familiarity on trust and adoption of recommendation agents," MIS Quarterly, 30:4, 941-960.

Kim, D.J., Ferrin, D.L., and Rao, H.R. 2008. "A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents," Decision Support Systems 44, 544-564.

Langheirnrich, M. 2001. "Privacy by Design — Principles of Privacy-Aware Ubiquitous Systems," Lecture Notes in Computer Science, 2201, 273-291.

Langheirnrich, M. 2002. "A privacy awareness system for ubiquitous computing environments," Lecture Notes in Computer Science, 2498, 237-245.

Malhotra, N.K., Kim, S.S., and Agarwal, J. 2004. “Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model,” Information Systems Research, 15:4, 336- 355.

McKnight, D.H, Carter, M., and Thatcher, J. B. 2011. “Trust in a specific technology: An investigation of its components and measures,” ACM Transactions on Management Information Systems, 2:2, 1-25.

McKnight, D.H., Choudhury, V., and Kacmar, C. 2002. “Developing and validating trust measures for e-commerce: An integrative typology,” Information Systems Research, 13:3, 334-359.

Mell, P., and Grance, T. 2011. “The NIST definition of cloud computing,” Cloud Computing and Government: Background, Benefits, Risks, 171-173.

Moore, G.C., and Benbasat, I. (1991). “Development of an Instrument to Measure the Perceptions of Adopting an Information Technology Innovation,” Information Systems Research*, 2*(3), 192-222.

Pavlou, P. A., Liang, H., and Xue, Y. 2007. “ Understanding and mitigating uncertainty in online exchange relationships: a principal-agent perspective,” MIS Quarterly, 31:1, 105-136.

Ryan, R.M., and Deci, E.L. 2000. “Intrinsic and Extrinsic Motivations: Classic Definitions and New Directions,” Contemporary Educational Psychology, 25:1, 54-67.

Sheldon, K.M., Turban, D.B., Brown, K. G., Barrick, M.R., and Judge, T.A. 2003. “Applying Self-Determination Theory To Organizational Research,” Personnel and Human Resources Management, 22, 357-393.

Shin, D.H. 2010. “Ubiquitous Computing Acceptance Model: End User Concern About Security, Privacy and Risk,” International Journal of Mobile Communications, 8:2, 169-186.

Smith, H.J., Dinev, T., and Xu, H. 2011. “Information privacy research: An interdisciplinary review,” MIS Quarterly, 35:4, 989-1015.

Soenens, B., Vansteenkiste, M., Lens, W., Luyckx, K., Goossens, L., Beyers, W., and Ryan, R.M. 2007. “Conceptualizing parental autonomy support: Adolescent perceptions of promotion of independence versus promotion of volitional functioning,” Development Psychology, 43, 633-646.